UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,042	11/19/2001	Steven Siong Cheak Mok	1085-PWH	2086

21034 7590 06/23/2005

IPSOLON LLP
805 SW BROADWAY, #2740
PORTLAND, OR 97205

EXAMINER	
HERRING, VIRGIL A	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/046,042	MOK, STEVEN SIONG CHEAK	
	Examiner	Art Unit	
	Virgil Herring	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 November 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on November 19, 2001. Claims 1-30 have been submitted for examination.

2. The examiner notes that the numbering of the claims of the disclosure does not conform to the requirements set forth in 37 CFR §1.75(f). For the purposes of examination, the claim numbering has been altered from the disclosure. The second claim numbered 26 will hence be referred to as claim 27. The claim labeled 27 will now be called claim 28, and is assumed to be dependent on claim 27 (because it further restricts the data archiving system first mentioned in claim 27). The claim labeled 28 will now be called claim 29. The claim labeled 29 will now be called claim 30. The applicant is requested to make these corrections in any updated submissions of the specification. The examiner further notes that the fees paid are based on 29 claims, rather than the 30 actually presented. The examiner kindly requests that the applicant clarify this point in the event that the examiner is misinterpreting the situation. For more information, please see Rule 1.126

3. Claims 1 through 30 have been rejected.

I. Drawings

4. The drawings are objected to because there are reference numbers for "black box" items which are not named and missing reference numbers for items discussed in

the specification in figures 2 (items: I/O logic actuator, means of monitoring, means of card readers and writers, means of card readers, means of handheld "RADAR"), 3 (item numbers 7, 10-12, 16), 4 (item numbers 7, 16-27), 5 (item numbers 7, 21, 22), 6a (item numbers 17-22), and 6b (item numbers 17-22). Also, the examiner notes an arrow directed from "Transmit Interrogation Signal" to both "Receive Interrogation Signal" and "Receive Response ID Number" in figure 8. Since figure 8 is a flowchart, it is improper to have two arrows directed out from one action box.

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 1, 32. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

6. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 9. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application.

7. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "16" has been used to designate both the "contact region

of the transponder card" (as shown in figure 3a and page 8, line 22) and the "terminal portion of the reader/writer" (page 10, line 24 of the specification). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

8. The drawings are additionally objected to because of minor informalities. The numbering of the drawings is not consistent throughout the disclosure (3 and 3a, compared to 6a and 6b). Also, the examiner notes that some of the drawings have title captions and some do not.

9. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

II. Abstract

10. Applicant is reminded of the proper language and format for an abstract of the disclosure:

> The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. In this case, the abstract includes well over 200 individual words, far exceeding the requirements. The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc. For example, starting a sentence with the phrase "Also disclosed is..." is unnecessary, because it is already implied that something is being disclosed by the application.

11. The abstract of the disclosure is objected to because it includes phrases that can be implied, is not limited to a single paragraph, and is not limited to 150 words. Correction is required. See MPEP § 608.01(b).

III. Specification

12. The layout of the specification is objected to. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

13. As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.

(b) CROSS-REFERENCE TO RELATED APPLICATIONS.

(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.

(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or

REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)

(e) BACKGROUND OF THE INVENTION.

(1) Field of the Invention.

(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(f) BRIEF SUMMARY OF THE INVENTION.

(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).

(h) DETAILED DESCRIPTION OF THE INVENTION.

(i) CLAIM OR CLAIMS (commencing on a separate sheet).

(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

14. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The examiner suggests the following new title: "Security System Including Identification Tracking Using RF Transponders."

15. A substitute specification, including the claims, is required pursuant to 37 CFR 1.125(a) because the specification is replete with errors, and contains numerous erroneous spellings which do not comport with United States practice. The most common problem noted is a series of missing figure reference numbers (for example,

page 12, lines 1, 5, 8, 9, 11, 12, 16, and 19). The copious number of misspellings includes: "authorised" and "authorisation" on pages 3, 14, 22, etc., "acces" on page 14, "metres" on page 14, "utilised" on page 18, and "realising" on page 18. Additionally, since the discussion of various parts of the figures is broken up, figure references should be used in addition to item references (an example of this is access point 30, shown in figures 1 and 2, but not mentioned in the detailed description until page 11). Also, the disclosure frequently uses the term "expiry" in a manner that its definition does not support (see in particular page 17, lines 7 and 9, and page 22, line 4).

16. A substitute specification must not contain new matter. The substitute specification must be submitted with markings showing all the changes relative to the immediate prior version of the specification of record. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. An accompanying clean version (without markings) and a statement that the substitute specification contains no new matter must also be supplied. Numbering the paragraphs of the specification of record is not considered a change that must be shown.

IV. Claim Objections

17. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

18. Misnumbered claims 26, 26, 27, 28, and 29 have been renumbered 26, 27, 28, 29, and 30 as discussed in paragraph 1 above.

19. Claims 14 and 15 are objected to because of the following informalities: spelling errors. Line 3 of claim 14: "authorised" should be "authorized." Line 2 of claim 15: "effect" should be "affect". Appropriate correction is required.

V. Claim Rejections - 35 USC § 101 & 112

20. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

21. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

22. Claim 23 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim is directed to neither a process nor a machine, but rather, overlaps the two statutory classes.

23. Claim 23 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter from a single statutory class which the applicant regards as the invention. The addition of method wording to a claim dependent on a system renders the claim language indefinite.

VI. Claim Rejections - 35 USC § 102

24. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

25. Claims 1-3, 5-10, 12, 21, and 24 are rejected under 35 U.S.C. 102(b) as being anticipated by Denne et al. (202).

26. Taking claim 1, for example, Denne et al. (202) disclose a security system for facilitating transponder carrier identification and tracking within a secure area comprising:

an RF transponder having a memory in which is stored a unique identifier; and

a transponder writer operable to send a replacement unique identifier to the transponder, the transponder replacing the identifier in the transponder memory with the replacement identifier. (Col. 2, Lines 17-35; Col. 10, Lines 29-40)

27. Denne et al. (202) discloses that the interrogator signals a specific transponder by transmitting the contents of page 0 of the transponder memory. They then go on to state that the interrogator is operable to send an instruction to change the contents of the memory, including page 0. Thus, the interrogator is changing the data used to identify the transponder, in other words, the identification code.

28. Examining claim 2, Denne et al. (202) disclose a security system according to claim 1 (above), wherein the transponder has a fixed unit identifier serving to identify the transponder, the fixed unit identifier being a separate identifier to the unique identifier. (Col. 1, Lines 62-68 & Col. 2, Lines 1-2)

29. Referring to claim 3, Denne et al. (202) disclose a security system according to claim 2 (above), wherein the unique identifier comprises an identity code. (Col. 1, Lines 62-68 & Col. 2, Lines 1-2)

30. Looking now at claim 5, Denne et al. (202) disclose a security system according to claim 3 (above), wherein the transponder includes a transmitter to transmit the unique identifier. (Col. 4, Lines 4-8)

31. Considering claim 6, Denne et al. (202) disclose a security system according to claim 5 (above), wherein the transmitter is a contactless transmitter operable to transmit RF signals. (Col. 1, Lines 11-15)

32. Regarding claim 7, Denne et al. (202) disclose a security system according to claim 5 (above), wherein the transmitter is a contact transmitter operable to send signals to a unit in contact with the transponder. (Col. 1, Lines 11-15; range = 0)

33. Concerning claim 8, Denne et al. (202) disclose a security system according to claim 3 (above), further comprising a transponder reader to receive from the transponder at least the unique identifier of the transponder. (Col. 10, Lines 55-63)

34. As for claim 9, Denne et al. (202) disclose a security system according to claim 8 (above), wherein the transponder reader interrogates the transponder and, in response

to the interrogation receives from the transponder at least the unique identifier of the transponder. (Col. 10, Lines 55-63)

35. With respect to claim 10, Denne et al. (202) disclose a security system according to claim 9 (above) wherein the transponder reader is mounted within the secure area and has a location code which provides information as to the location of the transponder reader. (Col. 1, Lines 26-29)

36. As per claim 12, Denne et al. (202) disclose a security system according to claim 9 (above), wherein the transponder reader has a predetermined interrogation range such that a transponder within the interrogation range will receive an interrogation signal from the reader and will respond thereto by sending its unique identifier. (Col. 1, Lines 11-15)

37. Referring now to claim 21, Denne et al. (202) disclose a security system according to claim 1 (above), wherein the carrier is selected from the group consisting of: personnel; a vehicle; and a hardware product. (Col. 1, Lines 22-25)

38. Turning now to claim 24, Denne et al. (202) disclose an RF transponder for use in a security system for facilitating transponder carrier identification and tracking within a secure area comprising:

a first memory in which is stored a replaceable unique identifier; and

a transmitter operable to send the unique identifier in response to an interrogation signal. (Col. 1, Lines 64-68; Col. 2, Lines 1-2)

VII. Claim Rejections - 35 USC § 103

39. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

40. Claim 4 is rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Tuttle (174).

41. As per claim 4, Denne et al. (202) do not expressly disclose a security system according to claim 1 (above), wherein the unique identifier is encrypted and assigned by a security processor.

42. However, Tuttle (174) discloses that an identification number can be encrypted before being written to the memory of the ID device. (Col. 5, Lines 24-26)

43. Denne et al. (202) and Tuttle (174) are analogous art because they are both from the field of secure identification of an individual.

44. At the time of the invention it would have been obvious to a person of ordinary skill in the art to modify Denne et al. (202) to encrypt the identification number stored in the memory of an identification transponder for use in a security system, in order to prevent an unauthorized user from using an identifier which does not conform to the encryption scheme being used. Further, it would be obvious that the security processor would assign the identification number, because if it did not, then it would not know whether the number was indeed valid. The motivation for combining Denne et al. (202) and Tuttle (174) would be to prevent an unauthorized user from stealing a transponder and using it, because he or she would not be able to generate a valid encrypted unique identifier. (Col. 5, Lines 41-45)

45. Claim 11 is rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Miller et al. (580).

46. As per claim 11, Denne et al. (202) do not expressly disclose a security system according to claim 10 (above), wherein the transponder reader is portable and operable within the secure area.

47. However, Miller et al. (580) disclose a portable data terminal that can be adapted for reading RF tags. (Col. 5, Lines 27-33; Figure 17)

48. Denne et al. (202) and Miller et al. (580) are analogous art because they are from the art of reading data from non-stationary sources.

49. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify Denne et al. (202) to include a portable RF transponder reader as taught by Miller et al. (580). The motivation for doing so would have been to create a transponder reader that is not limited to a single location. (Col. 5, Lines 27-33)

50. Claims 13-16 and 25 are rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Bowers et al. (134).

51. As per claim 13, Denne et al. (202) do not expressly disclose a security system according to claim 1 (above), further comprising a security processor having an access database setting out access parameters for the secure area and a carrier of a transponder, the security processor being operable to receive information from the

transponder reader comprising at least the unique identifier of an interrogated transponder and the location of the transponder reader.

52. However, Bowers et al. (134) disclose that a database record of articles marked with RF transponders can include a security field to identify any restrictions on the movement of the article. (Col. 17, Lines 50-61)

53. Denne et al. (202) and Bowers et al. (134) are analogous art because they both deal with the use of RF transponders.

54. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify Denne et al. (202) in such a way that a database of people carrying transponders would include information on what areas a specific person is allowed to enter, as taught by Bowers et al. (134). A data processing means (a "security processor") is implicit in this combination, because a database is, in reality, just a file on a computer, and has no capability to perform any actions without the associated computing hardware. The motivation for doing so would have been to devise a security system that controls access to certain areas. Under this system, some transponder carriers would be authorized to enter a restricted area, and some would not.

55. As per claim 14, Denne et al. (202) do not expressly disclose a security system according to claim 13 (above), wherein the security processor determines from consultation of the access database whether the carrier is authorized to be in the vicinity of the interrogating transponder reader and further determines what, if any, action needs to be taken.

56. However, it would have been obvious to combine Denne et al. (202) with Bowers et al. (134) in the manner described in ¶ 54. Further, it would be obvious to one skilled in the art of computing machinery that the security processor would have to consult the access database to determine if a carrier is authorized to be in the vicinity of the interrogating transponder reader. Without the access database, the security processor has no way of knowing who is authorized to be in what area, and thus has no function. In order to implement any kind of restrictions, the processor must consult with the database. It would also be obvious to one skilled in the art that the security processor would initiate some kind of action based on the information received from the access database. If the processor were to take no action, then there would be no purpose in even having it.

57. As per claim 15, Denne et al. (202) do not expressly disclose a security system according to claim 13 (above), further comprising an actuator controllable by the security processor to affect operation of a device in response to a condition determined by the security processor.

58. However, Bowers et al. (134) disclose zone interrogators that activate alarms if an article passing through the interrogation range is not properly marked in the database as being allowed to pass that point. (Col. 12, Lines 3-23)

59. As discussed in ¶ 54, it would have been obvious to combine Denne et al. (202) with Bowers et al. (134) to construct a security system including an access control database and security processor. It would be similarly obvious to include the alarm Bowers et al. (134) disclose in column 12, lines 3-23. The American Heritage® Dictionary defines an actuator to be "one that activates, especially a device responsible for actuating a mechanical device, such as one connected to a computer by a sensor link." For the security processor to have any function, it must perform some action after consulting the access database. Since the processor is really just a small chip inside a computer, the existence of some type of actuator in the system is implicit. Without an actuator connected in some way to the processor, the processor is unable to take any action based on a valid or invalid response from the access database.

60. As per claim 16, Denne et al. (202) do not expressly disclose a security system according to claim 15 (above), wherein the device activated by the actuator is selected from the group consisting of: an image capture device; an alarm; an alert system; a lock; an emergency door release; a speaker; and a communication device.

61. However, Bowers et al. (134) disclose a system in which a zone interrogator activates an alarm upon detection of an unauthorized transponder passing nearby. (Col. 12, Lines 3-23)

62. As discussed in ¶ 54, it would have been obvious to combine Denne et al. (202) with Bowers et al. (134) to construct a security system including an access control database, a security processor, and an alarm to inform personnel when someone is attempting unauthorized access to the secured area.

63. Finally, as per claim 25, Denne et al. (202) does not expressly disclose an RF transponder reader operable to send an interrogation signal to an RF transponder having a unique identifier and receive from the transponder in response to the interrogation signal, the unique identifier, the reader being operable to transmit the unique identifier to a security processor for identity verification.

64. However, as was shown in ¶ 54, it would have been obvious to combine Denne et al. (202) with Bowers et al. (134) to construct a security system including RF transponders, a transponder reader, and a security processor with access database. It would be obvious to one skilled in the art that the transponder reader would have some way to communicate with the security processor. Thus, an RF transponder reader operable to interrogate an RF transponder for its unique identifier, and to transmit that

unique identifier to the security processor would be covered by the combination of Denne et al. (202) and Bowers et al. (134)

65. Claims 17-20 and 30 are rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Ogasawara (015).

66. As per claim 17, Denne et al. (202) do not expressly disclose a security system according to claim 1 (above), wherein the transponder is configured as a card having a contact terminal.

67. However, Ogasawara (015) discloses a system in which "...a customer ID card 10 which might be implemented as a magnetic stripe card, a contact-type IC card, a contactless-type IC card or any other conventional form of ID card or ID tag that is able to be programmed with a customer identification number." (Col. 16, Lines 30-34)

68. Denne et al. (202) and Ogasawara (015) are analogous art because they are from the art of personal identification.

69. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify Denne et al. (202) in such a way that the transponder disclosed by Denne et al. (202) also includes a contact terminal as taught by Ogasawara (015). The motivation for doing so would have been to allow for a greater variety of ways in

which the data stored on the transponder could be read. In disclosing three specific ways (and allowing for an unnamed number of others) in which his customer ID card could be implemented, Ogasawara (015) implies that there are situations in which some types of cards have advantages over other types. This implies a need for a plurality of reading methods in a personal identification transponder.

70. As per claim 18, Denne et al. (202) do not expressly disclose a security system according to claim 17 (above), wherein a card reader/writer is provided having a contact region compatible with the card contact terminal, wherein the transponder is addressable by the card reader when the terminal and contact region are in contact with one another.

71. However, Ogasawara (015) discloses a system in which "a typical kiosk terminal 80 would comprise a card reader 82 which is configured to read a customer ID card 10..." (Col. 16, Lines 29-30)

72. The motivation for combining Denne et al. (202) with Ogasawara (015) is described in ¶ 69. The combination can be expanded to encompass Ogasawara's (015) card reader. The motivation for expanding the combination would simply be that a contact-type reader for a contact-type transponder is a logical necessity.

73. As per claim 19, Denne et al. (202) do not expressly disclose a security system according to claim 18 (above), wherein the card reader/writer is operable to write the replacement unique identifier to the transponder.

74. However, as previously discussed in ¶ 69, combining Denne et al. (202) with Ogasawara (015) is obvious. The system disclosed by Denne et al. (202) already includes writing a replacement unique identifier to the transponder memory (see ¶ 26). In the combination of Denne et al. (202) and Ogasawara (015), the reader/writer would still be interfacing with the transponder, and thus would still be operable to write a replacement unique identifier to the transponder memory.

75. As per claim 20, Denne et al. (202) do not expressly disclose a security system according to claim 18 (above), wherein the card reader/writer is integrated with an identification authentication device to as to authenticate the identity of a carrier of the transponder prior to writing a replacement unique identifier to the transponder of the carrier.

76. However, Ogasawara (015) discloses a system in which "if the customer has been issued with an ID card, inserting or swiping the ID card through the card reader 82 activates a digital camera 84 which takes a videographic image of the customer and transmits the videographic image, along with the customer ID, to either a system control unit 86 or a store server 88." (Col. 16, Lines 44-49)

77. The motivation and obviousness of combining Denne et al. (202) with Ogasawara (015) can be found in ¶ 69. It would be obvious to one skilled in the art of security to use the videographic image supplied by the digital camera to the server to verify the identity of a transponder carrier. As discussed in claim 19, the system disclosed by Denne et al. (202) already includes writing a new replacement identifier to the transponder, and the addition to Denne et al. (202) of identity verification is a logical inclusion from the teachings of Ogasawara (015).

78. As per claim 30, the motivation for combining Denne et al. (202) with Ogasawara (015) is explained in ¶ 69, as well as the reasons it would be obvious to do so. This combination includes all the hardware required for a method of identity verification comprising the steps of:

interrogating an RF transponder with an interrogation signal; (Denne et al., 202)

receiving a unique identifier from the transponder provided in response to the interrogation signal; (Denne et al., 202)

authenticating the identity of a user carrying the transponder; (Ogasawara, 015)

assigning a replacement unique identifier; and (Denne et al., 202)

writing the replacement unique identifier to the transponder to replace the received unique identifier. (Denne et al., 202)

79. Claim 22 is rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Nerlikar (981).

80. Denne et al. (202) do not expressly disclose a security system according to claim 1 (above), wherein the unique identifier has an expiry time after which the unique identifier is no longer valid.

81. However, Nerlikar (981) discloses a system in which authorization for a transponder to be in a restricted location, the authorization for that area can be changed dynamically, including expiring after a certain period of time. (Col. 13, Lines 57-68)

82. Denne et al. (202) and Nerlikar (981) are analogous art because they are both from the field of interrogating a transponder and allowing or denying its carrier access to a certain area.

83. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify Denne et al. (202) to include the imposition of a time limit on the validity of a transponder in the security system, as taught by Nerlikar (981). The motivation for doing so would have been to add another layer of security to the system, by requiring anyone with a transponder to check in and have it renewed at some point before or after its expiration time.

84. Claims 27-29 are rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Bowers et al. (134), and further in view of Nerlikar (981).

85. As per claim 27, Denne et al. (202) do not expressly disclose an RF transponder reader according to claim 25 (above), wherein the reader is integrated with a data archiving system. However, the motivation for combining Denne et al. (202) with Bowers et al. (134) is documented in ¶ 54. This combination does not expressly disclose an RF transponder reader according to claim 25, wherein the reader is integrated with a data archiving system.

86. However, Nerlikar (981) discloses that an RFID reader can be embedded in a personal digital assistant. (Col. 16, Lines 5-22) It is well known to those in the art that a personal digital assistant is a form of data archiving system. If the transponder reader is embedded in a data archiving system, then they are certainly integrated with one another.

87. Denne et al. (202), Bowers et al. (134), and Nerlikar (981) are analogous art because they all involve reading RF transponders.

88. At the time of the invention it would have been obvious to a person of ordinary skill in the art to modify the combination of Denne et al. (202) and Bowers et al. (134) to integrate a data archiving system with an RF transponder reader operable to interrogate transponders and communicate with a security processor, as taught by Nerlikar (981). The motivation for doing so would have been to provide a more versatile transponder reader that is small and portable.

89. As per claim 28, Denne et al. (202) does not expressly disclose an RF transponder reader according to claim 27 (above), wherein the data archiving system is a personal digital assistant. However, the motivation for combining Denne et al. (202) with Bowers et al. (134) to include a personal digital assistant as taught by Nerlikar (981) can be found in ¶ 88.

90. As per claim 29, Denne et al. (202) does not expressly disclose an RF transponder reader according to claim 25 (above), wherein the reader incorporates a cellular telephone system. However, the motivation for combining Denne et al. (202) with Bowers et al. (134) to create an RF transponder reader that can communicate with a security processor can be found in ¶ 54. This combination does not expressly disclose the incorporation of a cellular telephone system.

91. However, Nerlikar (981) discloses that a cellular telephone system (either the phone, the base station, or both) "...can have RFID readers of the present invention installed..." (Col. 10, Lines 66-67; Col. 11, Lines 1-5)

92. Denne et al. (202), Bowers et al. (134), and Nerlikar (981) are analogous art because they are all from the field of reading RF transponders.

93. At the time of the invention it would have been obvious to a person of ordinary skill in the art to modify the combination of Denne et al. (202) and Bowers et al. (134) to

incorporate a cellular phone system with an RF transponder reader operable to interrogate transponders for their identifiers as taught by Nerlikar (981), and to communicate that identifier to a security processor. The motivation for doing so would have been to employ the existing infrastructure of the cellular phone industry to allow interrogation of transponders using portable transponder readers.

94. Claim 26 is rejected under 35 U.S.C. 103(a) as being obvious over Denne et al. (202) in view of Bowers et al. (134), and further in view of Miller et al. (580)

95. As discussed in ¶ 54, it would have been obvious to combine Denne et al. (202) with Bowers et al. (134) to construct a security system including transponders, transponder readers, and a security processor. This combination does not expressly disclose an RF transponder reader according to claim 25 (above), wherein the reader is a portable unit.

96. However, Miller et al. (580) disclose a portable data terminal that can be adapted for reading RF tags. (Col. 5, Lines 27-33; Figure 17)

97. Denne et al. (202), Bowers et al. (134), and Miller et al. (580) area all analogous art because they are all in the field of security using RF transponders.

98. At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the combination of Denne et al. (202) and Bowers et al. (134) to create a security system including RF transponders, a security processor, and portable RF transponder readers as taught by Miller et al. (580). The motivation for doing so would have been to construct a security system in which the transponder interrogators are not limited to stationary positions, but rather, are portable (for instance, to be carried by security personnel).

VIII. Conclusion

99. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892 (included).

100. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday 8:00am-4:30pm.

101. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can normally be reached at (571) 272-3799 during similar hours. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100